IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT joegrubb5757@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 7:22mj66 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Scott M. Long, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with joegrubb5757@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC ("Google"), an electronic communications service and/or remote computing service provider headquartered at 1600 Amphitheater Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since 2002. I am currently assigned to the FBI Richmond, Virginia (VA), Field Office, Roanoke Resident Agency. As part of my duties as an FBI SA, I have

investigated criminal violations relating to transnational organized crime, complex financial crime and securities fraud, civil rights, human trafficking, violent gangs, drugs, and international terrorism. I have received training and gained experience in conducting investigations, interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, child pornography identification, computer evidence seizure and processing, and various other criminal laws and procedures.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience I am aware that 18 U.S.C. § 2261A(2) (Stalking) makes it a crime for whoever, with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person, uses the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce to engage in a course of conduct that places that person in reasonable fear of the death of or serious bodily injury . . . or causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to a person. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2261A(2) have been committed by Joe Miller GRUBB III. There is also probable cause to search the information described in Attachment A for evidence of these crimes as described in Attachment B.

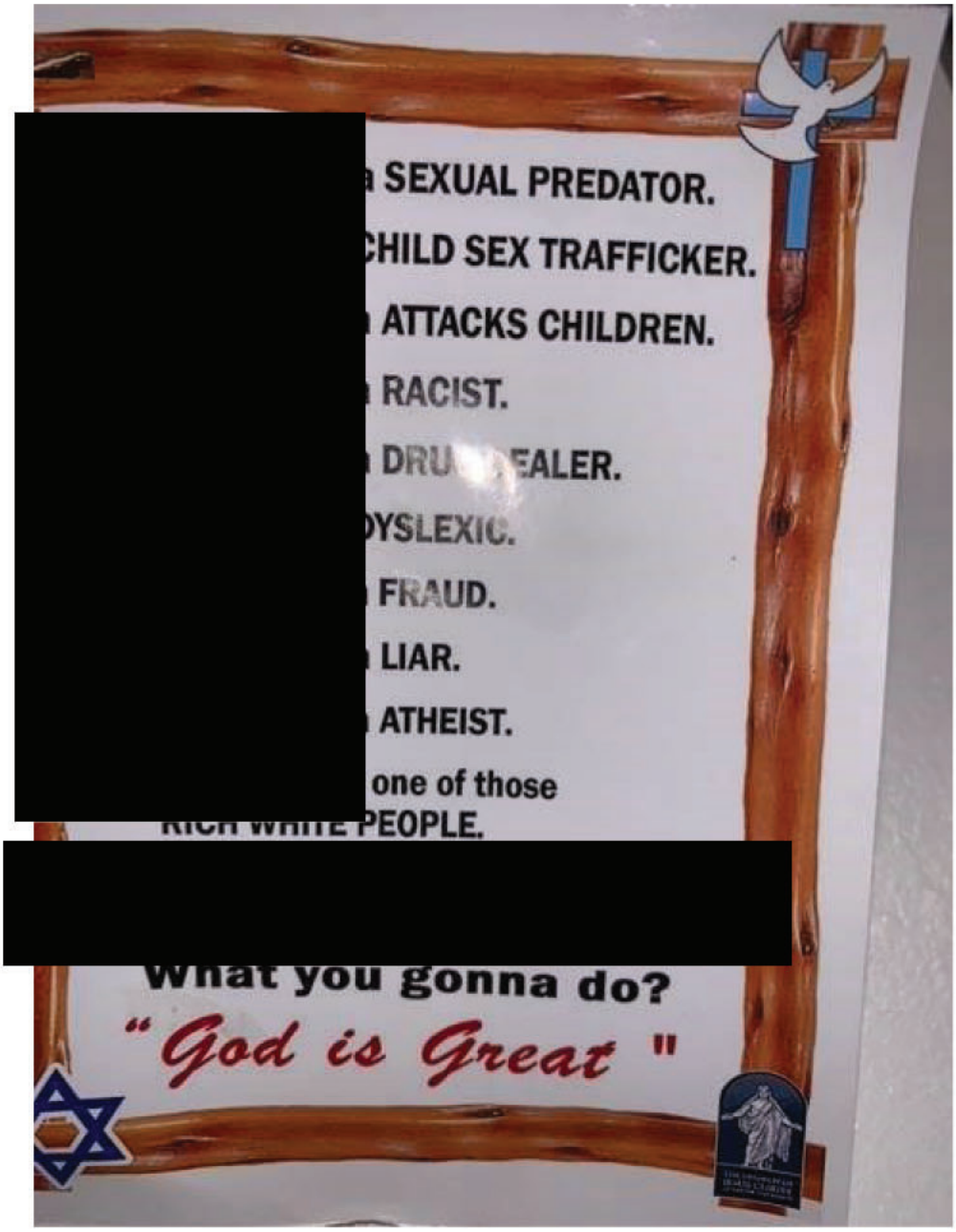
JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On October 11, 2021, an email was sent from the email address joegrubb5757@gmail.com to five employees of American National Bank (AMNB) with the subject line: "[redacted] sexual abuse" at approximately 11:32 P,M EST. The email stated: "See pics. Video to follow. Think people want to invest with you now. Respectfully, Joe M. Grubb joegrubb5757@gmail.com" Inserted in the body of the email were three photographs, the first of which was a list of allegations against [redacted] (see below photo A)



(Photo A - first photograph in the email dated 10/11/2021)

7. The second photograph in the email was of the Captain America shield logo, and the third photograph was of GRUBB standing next to the banner above (see below photo B).

(Photo B - third photograph in the email dated 10/11/2021).

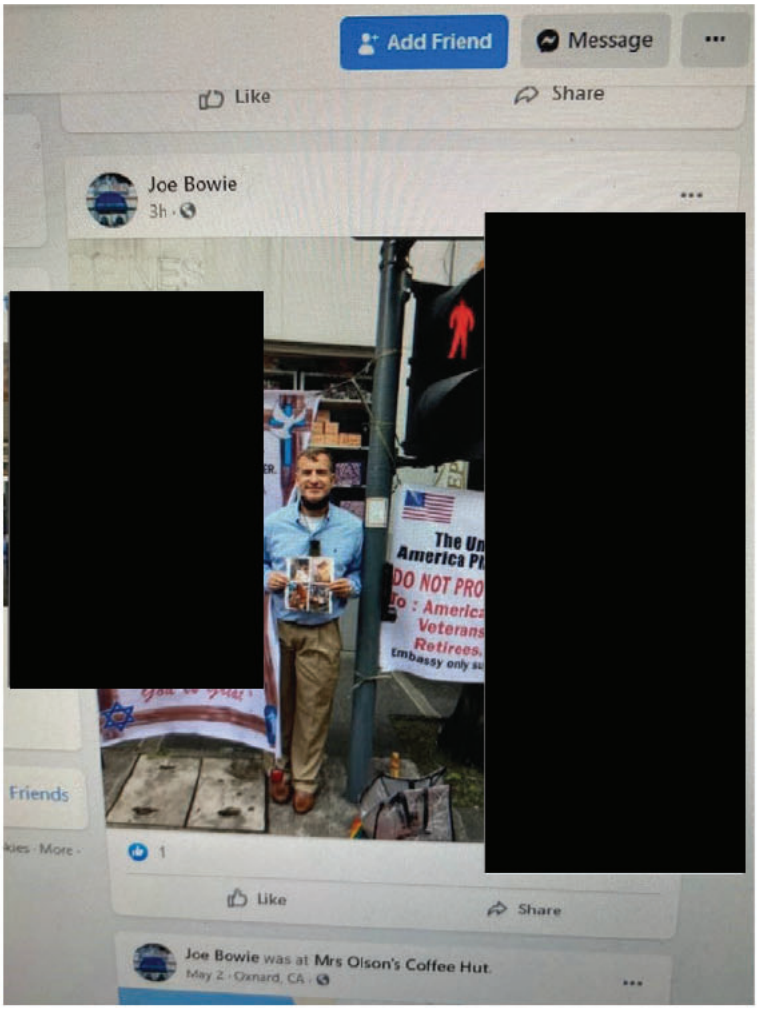
8. Investigation identified WITNESS 1, who identified GRUBB as the individual pictured in Photo B above, and confirmed GRUBB's use of the email address

joegrubb5757@gmail.com. WITNESS 1 also stated GRUBB was in Manila, Philippines at the time these photographs were taken and the emails set forth above were sent.

9. Additional emails were sent on the same day by GRUBB (using the same gmail account) to several AMNB employees with subject lines that included," Video sound clips [redacted] "Video [redacted] "Sound/have over 300 hours of this creep.", and "[redacted] sound". These emails contained video attachments, one of which showed an individual walking around a room, opening an exterior door, and then the sound of street noise can be heard. There is no discernable, audible conversation in the video.

10. [redacted] is a [redacted] at AMNB and lives at the address listed in the photos posted by GRUBB. This residence is adjacent to GRUBB's U.S. residence address in Roanoke, Virginia. [redacted] knows GRUBB from occasional, cordial interactions as neighbors. [redacted] cannot recall any negative interactions with GRUBB in the past [redacted] direct supervisor at AMNB and the bank's Chief Financial Officer were recipients of GRUBB's emails.

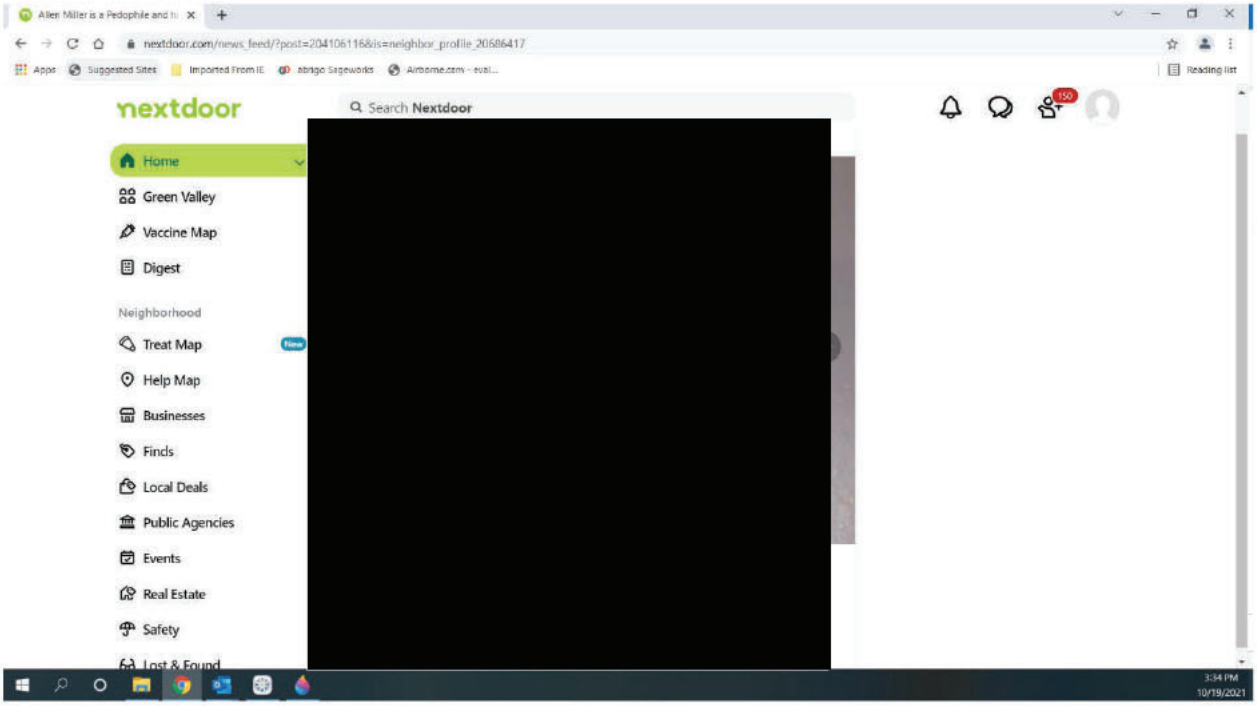
11. On October 17, 2021, a photograph similar to Photos A and B, above, was posted under the name Joe Bowie on Facebook (see below Screenshot C). WITNESS 1 stated that Joe Bowie is an alias that GRUBB uses for posting on Facebook. Facebook is an electronic communication service and facility of interstate commerce.



Screenshot C Grubb post as Joe Bowie on Facebook on 10/17/2021.

12. On October 19, 2021, [redacted] the spouse of [redacted] saw a post on the social media website Nextdoor containing three photographs, a picture of [redacted] the banner in Photo A and a picture similar to the Facebook post shown in Screenshot C. Nextdoor is an electronic communication service and facility of interstate commerce. The Nextdoor post was placed in the general section of the Greater Deyerle neighborhood page, the neighborhood [redacted] lives in, and titled "Pedophile [redacted]". The post ends with "CPT Joe Grubb". The post

was made on October 11, 2021 under the name Joe David. WITNESS 1 stated this account was associated with GRUBB. Below is a screen capture of part of the Nextdoor post:



Screenshot C of Nextdoor post.

13. On or about October 25, 2021, five branches of AMNB received letters postmarked October 23, 2021 with a return address of or similar to "CPT Joe Grubb [redacted] Roanoke, VA 24018". These letters contained a sheet of paper with the same or similar picture referenced above in Photo A.

14. Further investigation identified WITNESS 2, who approximately a week prior to October 23, 2021 received a package from GRUBB that contained numerous letters. GRUBB asked WITNESS 2 to mail the letters for him in the United States. WITNESS 2, who lives in Maryland, mailed the letters for GRUBB without any knowledge of what was inside.

15. On or about October 30, 2021, twenty letters either postmarked October 27, 2021 or missing postmarks were either delivered or scheduled to be delivered to neighbors of [redacted] These letters were the same as or similar to the letters sent to AMNB.

16. On or about October 31, 2021, GRUBB told WITNESS 1 that if he ever came back to the United States, he would kill [redacted] GRUBB medically retired from the U.S. Army in 2016. GRUBB was diagnosed with Post Traumatic Stress Disorder (PTSD) and with bi-polar disorder while at Fort Knox in approximately 2015.

17. [redacted] have endured substantial emotional distress due to the conduct of GRUBB and they fear for their lives. They are worried about individuals who may believe GRUBB's social media posts or letters and act on his statement from Photo A "What you gonna do?" They also feared what GRUBB might do if he returned to the United States.

18. On or about December 22, 2021, GRUBB sent over sixty similar letters via FedEx to numerous individuals, businesses, government offices and other entities to include the Hell's Angels Motorcycle Club.

19. In one of the letters sent via FedEx on or about December 22, 2021 addressed to a business in the Roanoke, Virginia area, GRUBB threatens to kill one of the employees of the business.

20. On January 4, 2022, the Philippine Bureau of Immigration arrested GRUBB.

21. A preservation request was sent and a Grand Jury subpoena was served on Google on June 7, 2022 and Google Reference Number 19605656 was assigned to this matter

BACKGROUND CONCERNING GOOGLE

22. Google is a United States company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

23. In addition, Google offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device, and a Google Account is required for certain functionalities on these devices.

24. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account.

25. Google advertises its services as "One Account. All of Google working for you." Once logged into a Google Account, a user can connect to Google's full suite of services offered to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

26. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

27. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

28. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more

through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

29. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

30. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one

New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

31. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. For example, users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. Users can upload photos and videos to Gmail directly from Google Photos. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account.

32. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

33. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the

account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

34. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

35. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. These records may establish who sent the threatening and harassing emails, and provide access to pictures used and may establish connections with other threatening or harassing communications.

36. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal

activity, including to communicate and facilitate the offenses under investigation. Thus, stored communications and files connected to a Google Account may provide direct evidence of the offenses under investigation.

37. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

38. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (*e.g.,* information indicating a plan to commit a crime), or consciousness of guilt (*e.g.,* deleting account information in an effort to conceal evidence from law enforcement).

39. Other information connected to the use of a Google account may lead to the discovery of additional evidence. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of instrumentalities of the crimes under investigation.

40. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

CONCLUSION

41. Based on the forgoing, I request that the Court issue the proposed search warrant.

42. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Scott M. Long
Scott M. Long
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on June 30, 2022

Robert S. Ballou
Honorable Robert S. Ballou
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with joegrubb5757@gmail.com ("the Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on June 7, 2022 with Google Reference Number 19605656, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from October 1, 2021 to January 4, 2021, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
6. Length of service (including start date and creation IP) and types of service utilized;
7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs

d. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails.

e. Any records pertaining to the user's contacts, including: address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history.

f. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.

g. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.

h. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides), including: files, folders, media, notes and note titles, lists, and other data uploaded, created, stored, or shared with the account including drafts and deleted records; the creation and change history of each record; accounts with access to or which previously accessed each record; any location, device, other Google service (such as Google Classroom or Google Group), or third party application associated with each record; and all associated logs, including access logs and IP addresses, of each record.

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and instrumentalities of violations of 18 U.S.C. § 2261A(2) (Stalking) since October 1, 2021, involving the user ID identified on Attachment A, information pertaining to the following matters:

a. Communications regarding threats, intimidation, harassment and violence against [redacted] or any other person;

b. Evidence indicating how and when the Account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

c. Evidence indicating the Account owner's state of mind as it relates to the crime under investigation;

d. The identity of the person(s) who created or used the Account, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC ("Google"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature